

[| NODIS Library](#) | [Organization and Administration\(1000s\)](#) | [Search](#) |

NASA Procedural Requirements

COMPLIANCE IS MANDATORY**NPR 1600.1A**Effective Date: August 12,
2013Expiration Date: August 12,
2018[Printable Format \(PDF\)](#)

Request Notification of Change

 (NASA Only)

Subject: NASA Security Program Procedural Requirements

Responsible Office: Office of Protective Services[| TOC](#) | [Preface](#) | [Chapter1](#) | [Chapter2](#) | [Chapter3](#) | [Chapter4](#) | [Chapter5](#) | [Chapter6](#) | [AppendixA](#)
[| AppendixB](#) | [AppendixC](#) | [AppendixD](#) | [AppendixE](#) | [AppendixF](#) | [AppendixG](#) | [AppendixH](#) | [ALL](#)

Chapter 2. Security Operations

2.1 Security Controls at NASA Centers

2.1.1 Procedures shall be implemented to ensure only authorized personnel are admitted to NASA controlled, owned, and leased property.

2.1.2 Each Center shall apply and maintain appropriate physical security measures necessary to provide for protection of persons, missions, information, and property as promulgated in NPR 1620.3A, Physical Security Requirements for NASA Facilities and Property.

2.1.3 The maintenance of a controlled perimeter and entry access control points (ACPs) are fundamental to NASA's security-in-depth approach to physical security.

2.1.3.1 All Center perimeter entry ACPs open to traffic shall be staffed by armed, uniformed Security Police Officer (SPO)/Security Officer (SO) personnel at all times. The SPO/SO will:

- a. Validate the personnel identification and access eligibility of all personnel entering NASA property by visually examining Federal identification or locally produced, temporary visitor identification or passes.
- b. Visually match the photograph with the face of the person presenting the identification.
- c. Authenticate identification cards and access using automated means where available.
- d. Assess entering vehicles for obvious security concerns.

2.1.3.2 To prevent unauthorized access to critical areas, information, or personnel, additional access control measures, including the use of unarmed personnel, electronic access equipment, and passive and active barriers may be established at individually designated ACPs, security areas, and facilities within the Center.

2.1.3.3 Each Center shall be responsible for the procurement, installation, management, and maintenance of all Center premise access control equipment, integrated intrusion detection, closed-circuit video equipment, and any peripheral equipment.

2.1.3.4 SPO/SOs shall be used throughout the Center to provide traffic safety, detect and deter criminal conduct, enforce security rules and policies, detect unauthorized personnel, act as first responders to critical incidents, establish emergency or temporary control points, respond to calls for assistance, and perform other duties as determined by the CCPS/CCS.

2.1.4 Photography at NASA Facilities.

2.1.4.1 Center Directors, in coordination with the CCPS/CCS and the Center Office of the Chief Counsel, shall establish and implement an individual Center photography policy for the general and public access areas consistent with existing security conditions.

2.1.4.2 Photography is prohibited in Limited areas, Exclusion areas, and within NCI facilities without prior approval of the CCPS/CCS.

2.2 Inspection of Persons and Property

2.2.1 General.

2.2.1.1 Consistent with NASA's requirement to ensure appropriate protection for personnel, property, and facilities, NASA reserves the right to conduct an inspection of any person and property in his/her possession as a condition of admission to, continued presence on, or upon exit from any NASA facility. Implementation of requirements, policy, and procedures for all aspects of this program shall be in accordance with 14 C.F.R. Part 1204, subpart 10. NPR 1620.3, Physical Security Requirements for NASA Facilities and Property, Appendix C addresses items prohibited from NASA facilities. Where NASA facilities are located on a military installation or an area of concurrent/proprietary jurisdiction, NASA personnel are subject to their policies and procedures.

2.2.1.2 All entrances to NASA real property or installations shall be conspicuously posted with the following notices:

- a. "CONSENT TO INSPECTION: Your entry into, continued presence on, or exit from this installation is contingent upon your consent to inspection of person and property."
- b. "UNAUTHORIZED INTRODUCTION OF WEAPONS OR DANGEROUS MATERIALS IS PROHIBITED: Unless specifically authorized by NASA, you may not carry, transport, introduce, store, or use firearms or other dangerous weapons, explosives or other incendiary devices, or other dangerous instrument or material likely to produce substantial injury or damage to persons or property."

2.2.2 SPO/SOs shall be trained on how to perform inspections and, with appropriate training, may use inspection tools and detection devices (mirrors, x-ray, and other sensing devices) and/or canines, as necessary.

2.2.2.1 Training for security personnel conducting searches shall include:

- a. Appropriate search techniques for the type of vehicle being searched.
- b. Key locations where devices or other contraband may be secreted.
- c. Procedures for confiscating illegal or dangerous items, detaining of individuals, and referring incidents to the NASA OIG or appropriate external law enforcement.

2.2.2.2 Such inspections shall be conducted in accordance with the following guidelines:

- a. Consent to Inspection Notices shall be prominently posted at entrances to NASA Centers and Facilities. Language for these notices is contained in 14 C.F.R. §1204.1003, Subpart 10.
- b. Only NASA security personnel or members of the installation's uniformed security force will conduct inspections. Such inspections will be conducted in accordance with guidelines established by the AA, OPS.
- c. Prior to undertaking an inspection, security personnel not in uniform shall present their NASA credentials to the subject of the inspection.
- d. If, during inspection, an individual is found to be in unauthorized possession of items believed to represent a threat to the safety or security of the Center (e.g., CNSI, weapons, drugs, or explosives), or other prohibited items described in NPR 1620.3A, Physical Security Requirements for NASA Facilities and Property, Appendix C, the items shall be confiscated, and the individual will be denied admission to or be escorted from the Center or detained at the scene as directed by the CCPS/CCS or his/her designee. The NASA OIG or appropriate local law enforcement authorities will be notified immediately.
- e. If, during an inspection conducted pursuant to this subpart, an individual is in possession of U.S. Government property without proper authorization, that person will be required to relinquish the property to the security representative pending a determination on the proper authorization for the possession of the property or its removal from the installation. The individual relinquishing the property will be provided with a receipt for the property.

2.3 Violations of Security Requirements

Anyone who willfully violates, attempts to violate, or conspires to violate any regulation or order involving NASA security requirements is subject to disciplinary action up to and including termination of employment and/or possible prosecution under 18 U.S.C. § 799, which provides fines or imprisonment for not more than one year, or both.

2.4 Denial of Access

2.4.1 To address immediate security and safety issues, the AA, OPS has delegated authority to the CCPS/CCS for denial of access. CCPS/CCS, Center Directors, and the Headquarters Operations Director or their designees may

order the temporary denial of access or removal from NASA facilities/resources of any person who violates NASA security requirements, national security regulations, or whose continued presence on NASA property constitutes a security or safety risk to persons or property.

2.4.2 The foregoing is a denial of access and is distinct from suspension or removal from Federal employment of Federal civil servants, which is governed by 5 C.F.R. Parts 315, 731, 752, or 359 and in coordination with the Center Office of Human Capital Management (OHCM) and Center OCC/OGC.

2.5 Imminent Security Threat or Safety Risk

2.5.1 The CCPS/CCS, Center Directors, and the Headquarters Operations Director or their designees shall order the temporary removal and/or denial of access to all NASA facilities of any person who violates NASA security requirements and whose continued presence on NASA property constitutes an imminent security threat or safety risk to persons or property. Circumstances of removal and/or denial of access will be articulated in a report to become a matter of official record.

2.5.2 Civil Service Employees.

2.5.2.1 Immediately upon taking such action, the CCPS/CCS will notify the Center Director, Center OHCM, and Center OGC of the reasons for the decision to temporarily deny access or remove from NASA facilities/resources any civil service employee. As soon as reasonably possible, the CCPS/CCS will notify the AA, OPS. If no imminent security threat or safety risk exists, any contemplated temporary denial of access shall be advised and commented upon prior to action by Center OHCM and Center OCC/OGC. Any non-concurrence requires Center Director decision or notification.

2.5.2.2 Upon notification by the CCPS/CCS, as designee, of the temporary removal or denial of access of the civil service employee, the Center OHCM in consultation with OCC/OGC shall then determine the appropriate access status and any other employment limitations of the civil service employee. The employee may continue to be denied access until this status is finalized.

2.5.3 Contractor and Non-NASA Employees.

2.5.3.1 For contractor and non-NASA employees (e.g., visitors and guests) denied access, and immediately after denying access, the CCPS/CCS, as designee, shall notify the appropriate Government sponsor and contracting officer of the reasons for the decision to temporarily deny the individual's access to or remove them from the Center.

2.5.3.2 The CCPS/CCS shall notify the non-NASA employee who is denied access in writing of the reason for the temporary removal or denial of access and of the Denial of Access Reconsideration Process. Should the individual elect not to request reconsideration/appeal, the decision may become final. In his discretion, the AA, OPS may reconsider any denial of an access decision.

2.5.3.3 The CCPS/CCS shall conduct a new determination in consideration of the security violation to determine continued access eligibility of the employee consistent with the HSPD-12 credentialing standards listed in NPR 1600.3, Personnel Security Section 2.16.

2.5.3.4 Should the CCPS/CCS make a final determination to deny access, the individual may initiate the Denial of Access Reconsideration Process. This shall occur in accordance with NPR 1600.3, Personnel Security Section 2.17.

2.5.3.5 If the non-NASA employee denied access declines to appeal, either through communicating in writing or time for the appeal has expired, the original determination will be final. During the reconsideration process the individual is not granted access to any NASA facility unless coordinated with the CCPS/CCS.

2.5.3.6 Upon resignation, termination of employment, or release of the non-NASA employee by his/her employer or sponsor, the reconsideration/appeal process will otherwise continue, per NPR 1600.3, Personnel Security Section 2.17.

2.6 Denial of Access - Security Considerations

2.6.1 As designee of the AA, OPS, the CCPS/CCS shall take appropriate security measures to monitor, control, and restrict physical and logical access by individuals to the Center. These measures may include:

- a. Recovery and confiscation of NASA issued access badge(s) and IT resources.
- b. Posting of denial of access information at all Center access locations.
- c. Notification to Center IT resources to deny IT access.
- d. Suspension of access to CNSI.
- e. Notification to appropriate supervisory personnel referencing denial of access.

f. Inspections and securing of the individual's Center work space.

g. Notification to other NASA Centers and the AA, OPS.

2.7 NASA Security Areas

2.7.1 Types of NASA Security Areas.

2.7.1.1 NASA Controlled Area (formerly known as "Restricted Area") as defined in 14 C.F.R. Part 1203a. A Controlled Area is a physical area, including buildings or facilities, in which security measures are taken to safeguard and control access to property and hazardous materials or other sensitive material or to protect operations that are vital to accomplishing the mission assigned to a Center or Component Facility. The Controlled Area shall have a clearly defined perimeter, but perimeter physical barriers are not required.

a. Personnel within the area shall be responsible for challenging all persons who may lack appropriate access authority.

2.7.1.2 NASA Limited Area as defined in 14 C.F.R. Part 1203a. A Limited Area is a physical area in which security measures are taken to safeguard or control access to classified material or unclassified property warranting special protection or property and hazardous materials or to protect operations that are vital to the accomplishment of the mission assigned to a Center or Component Facility. A Limited Area shall also have a clearly defined perimeter; but where it differs from a Controlled Area is that permanent physical barriers and access control devices, including walls and doors with locks or access devices are implemented to assist occupants in keeping out unauthorized personnel. All facilities designated as NASA Critical Infrastructure (NCI) or key resources will be designated at minimum as "Limited" areas.

a. During working hours, personnel within the area will be responsible for challenging all persons who may lack appropriate access authority.

b. Sensitive material, property, and hazardous material can be stored in this area in approved containers. All CNSI material will be secured during non-working hours or when no cleared personnel are present in GSA approved security containers or other methods approved by the CCPS/CCS. c. When the Limited Area is not in use, access through the access control devices (i.e., keys, combinations to mechanical/electronic cipher locks, and badge reader controls) will be limited to authorized personnel. To prevent unauthorized access to such property, visitors will be escorted or other internal restrictions implemented, as determined by the CCPS/CCS.

2.7.1.3 NASA Exclusion Area (formerly known as a "Closed Area") as defined in 14 C.F.R. Part 1203a. An Exclusion Area is a permanent facility dedicated solely for safeguarding and use of CNSI. It is used when vaults are unsuitable or impractical and where entry to the area alone provides visible or audible access to classified material.

a. To prevent unauthorized access to an Exclusion Area, visitors will be escorted or other internal restrictions implemented, as determined by the CCPS/CCS.

2.7.2 Establishment, Maintenance, and Revocation.

2.7.2.1 Establishment.

2.7.2.1.1 Center Directors, Director of Headquarters Operations, or their designee (the designee is CCPS/CCS unless otherwise specified), and the AA, OPS shall establish, maintain, and protect such areas designated as NASA Controlled (formerly known as a "Restricted Area"), NASA Limited, or NASA Exclusion (formerly known as a "Closed Area") per the foregoing definitions and criteria.

a. Only the AA, OPS or the CCPS/CCS will establish an area functioning for the protection, use and storage of CNSI.

b. Only a coordinating office or the AA, OPS will establish a Special Access Program Facility (SAPF) or Sensitive Compartmented Information Facility (SCIF) based on legal authority, Memorandum of Agreement (MOA) or Memorandum of Understanding (MOU) with the Cognizant Security Authority and as promulgated in NPD 1600.4, National Security Programs.

2.7.2.2 Maintenance.

2.7.2.2.1 Security measures shall vary according to individual situations; however, the following minimum-security measures will be taken in all security areas:

a. Post appropriate signage at entrances and at intervals along the perimeter of the designated area, for the facility to provide reasonable notice to persons that the area is a security area. SAPFs and SCIFs are not required to use identifying signs due to Operations Security (OPSEC) concerns.

(1) Outdoor signs are metal, measuring approximately 40.64 cm/16 inches high and 50.8 cm/20 inches wide.

(2) Indoor signs are of cardboard or foam board, measuring approximately 22.86 cm/9 inches high and 12 inches wide.

b. Signage shall be ordered through Center supply sources for NASA Forms. Available signage includes:

(1) Controlled Area Sign (Outdoors), NASA Form 1506

(2) Controlled Area Sign (Indoors), NASA Form 1506A

(3) Limited Area Sign (Outdoors), NASA Form 1507

(4) Limited Area Sign (Indoors), NASA Form 1507A

(5) Exclusion Area Sign (Outdoors), NASA Form 1508

(6) Exclusion Area Sign (Indoors), NASA Form 1508A

c. Regulate authorized personnel entry and movement within the area; deny entry to unauthorized persons or material.

2.7.2.3 Revocation.

Once the need for a security area no longer exists, the area must return to normal non-secure area procedures as soon as practical.

2.7.3 Access.

2.7.3.1 Only those NASA employees, contractors, and visitors who need access and who meet the following access criteria shall enter a security area unescorted. All other individuals requiring access must be continually escorted by authorized NASA employees or NASA contractors.

2.7.3.2 To enter a NASA Controlled Area (formerly known as "Restricted Area") unescorted, individuals must undergo the appropriate investigation or training procedures required for that area as established by the individual Center or program. When an investigation is required, at a minimum, a National Agency Check with Inquiries (NACI) shall be initiated for civil service employees and for non-NASA personnel.

2.7.3.3 To enter a NASA Limited Area unescorted, individuals must have a need-to-know and a security clearance equal to the classification of material in the area or, at a minimum, a favorably adjudicated NACI for areas with unclassified information and material.

2.7.3.4 To enter a NASA Exclusion Area (formerly known as "Closed Area") unescorted, individuals must have a need-to-know and a security clearance equal to the classification of the material in the area.

2.7.3.5 Center Directors and the AA, OPS shall rescind previously granted authorizations to enter NASA Security Areas when an individual's clearance and need-to-know are no longer justified, their presence threatens the security or safety of the property, or when access is no longer required for official purposes.

2.8 Standards for Secure Conference Rooms

2.8.1 When established as permanent facilities, NASA Secure Conference Rooms shall meet security standards outlined in Director National Intelligence (DNI) Intelligence Community Directive (ICD) Number 705.

2.8.2 At a minimum, NASA Secure Conference Rooms shall be identified as NASA Limited Areas.

2.8.3 The following measures shall be taken when infrequent classified meetings are held in rooms not configured in accordance with ICD 705.

2.8.3.1 Meetings shall be limited to collateral Secret or below.

2.8.3.2 Meetings shall not be regularly scheduled or re-occurring meetings.

2.8.3.3 Positive access control shall be implemented, and personnel security clearances of all attendees will be validated.

2.8.3.4 A Security Specialist shall conduct a visual inspection and establish security procedures for the meeting.

2.8.4 Special Cases.

2.8.4.1 The preceding specifications do not apply to conference areas in which the level of security exceeds the collateral Secret level.

2.8.4.2 For these areas, guidance on additional requirements will be provided by the CCPS on a case-by-case basis. 2.8.4.3 The AA, OPS or CCPS/CCS shall be contacted for any interpretation of these specifications.

2.9 Technical Surveillance Countermeasures (TSCM)

2.9.1 TSCM Program.

The AA, OPS is responsible for the NASA TSCM program. The program shall be consistent with ICD 702 Technical Surveillance Countermeasures. All matters pertaining to the conduct of TSCM activities throughout the Agency will be directed and coordinated through the AA, OPS.

2.10 National Terrorism Advisory System (NTAS)

2.10.1 General.

2.10.1.1 The protection of NASA employees and assets from acts of terrorism at NASA-owned or leased property in the United States or abroad shall be given priority, especially during periods of heightened threat.

2.10.1.2 Although absolute protection against such acts is not possible, protective procedures shall be based on the threat level and reflect a balance among the degrees of protection required, the resources available, Agency mission requirements, and other pertinent factors.

2.10.1.3 In addition to assistance from OPS, the Center shall obtain support from representatives such as the Department of Defense (DoD), Federal Bureau of Investigation (FBI), Department of State, NASA Office of Inspector General (OIG), and state and municipal law enforcement agencies.

2.11 NASA National Terrorism Advisory System (NTAS) Program

2.11.1 This section explains the establishment of the NASA NTAS program which is designed to meet the requirements of the NTAS developed and implemented by the Department of Homeland Security (DHS).

2.11.2 NASA NTAS and associated actions are outlined in Appendix D, NASA NTAS Actions.

2.11.3 NASA Centers hosting military organizations as tenants, residing as a tenant on a military installation, or situated contiguous to a military installation shall establish mutually agreed upon notification systems for ensuring DoD's use of ALPHA designators under the DoD Force Protection Condition concept are understood and integrated into the Center's threat condition warning system.

2.11.4 NASA's alert system recognizes and utilizes the alert type structure of the DHS NTAS to provide for a greater consistency to threat reactions at both the national and at the Agency level.

2.11.4.1 The alert system types range from "No Current Alerts" (normal operating security policy), "Elevated Threat Alert," and "Imminent Threat Alert."

2.11.4.2 The alert system is intended to standardize terms and establish standardized security measures that can be initiated by the AA, OPS and Center Directors through the Agency-wide emergency notification system.

2.11.4.3 The AA, OPS shall initiate, modify, or rescind NASA-wide NTAS.

2.11.4.3.1 The AA, OPS shall monitor the threat status in the Agency and maintain close liaison with the DHS and national-level intelligence and security agencies for timely and accurate threat information.

2.11.4.4 Center Directors and CCPS/CCS shall implement threat mitigation measures initiated by the AA, OPS and may implement additional measures for their Center based on the local threat situation. They will not lower or rescind a threat mitigation action initiated by the AA, OPS.

2.11.4.5 The CCPS/CCS shall maintain close liaison with the local FBI offices and local law enforcement agencies for threat information.

2.12 Security Threat and Incident Reporting

2.12.1 General.

2.12.1.1 All Centers shall implement a security threat and incident reporting system, as required by NPD 1600.2, NASA Security Policy.

2.12.1.2 The system's purpose is to keep the Agency's senior management officials advised on a timely basis of serious security-related incidents or threats that may affect the NASA mission.

2.12.1.3 After advising Center senior management officials, CCPS/CCS reports shall be forwarded expeditiously to the AA, OPS. Refer to Appendix E, NASA Serious Incident Report for format.

2.12.2 The CCPS/CCS ensures that incidents are reported to the AA, OPS and followed up with a detailed situation report that describes the incident.

2.12.3 Any type of incident that might have Agency security implications shall be reported to the AA, OPS in a timely manner, including but not limited to the following:

- a. All crimes or incidents at a Center requiring notification of NASA OIG, the Federal Bureau of Investigation (FBI), Drug Enforcement Agency (DEA), Bureau of Alcohol, Tobacco, Firearms, and Explosive (ATF), or local law enforcement.
- b. Suspected Espionage (reported through appropriate classified Center Counterintelligence (CI) channels).
- c. Suspected Sabotage (reported through appropriate classified Center CI channels).
- d. Suspected terrorist activity (e.g., surveillance, photography, attempted penetrations, and unusual requests for information (reported through appropriate classified Center CI channels)).
- e. Bombing incidents, including bomb threats and necessary responses, which severely impact Center activities.
- f. Actual or planned demonstrations or strikes.
- g. All weapons discharges, including unintentional discharges, or other violent acts. Refer to Appendix H, Discharge of Firearms. Planned and pre-approved scientific or experimental discharges do not require reporting.
- h. All incidents (mishaps and close calls) that involve a fatality, the need for professional medical attention, or damage to NASA facilities or equipment and meet NPR 8621.1, NASA Procedural Requirements for Mishap and Close Call Reporting, Investigating, and Recordkeeping classification criteria shall be reported and processed in accordance with NPR 8621.1, NASA Procedural Requirements for Mishap and Close Call Reporting, Investigating, and Recordkeeping.
- i. All incidents occurring on NASA property that result in the death of a person. (NOTE: Deaths on NASA property shall be reported to the Center NASA Safety Office in accordance with NPR 8621.1, NASA Procedural Requirements for Mishap and Close Call Reporting, Investigating, and Recordkeeping).
- j. A security-related incident that would be of concern to NASA management due to a potential for public interest, embarrassment, or occurrence at other NASA facilities and/or in which the media has become involved and publicity is anticipated.
- k. An adverse event in an automated systems environment that would be of concern to NASA management due to a potential for public interest, embarrassment, or occurrence at other NASA facilities. These incidents shall include unauthorized access, theft, interruption of computer/network services or protective controls, damage, disaster, or discovery of a new vulnerability.
- l. Threats against NASA property.
- m. Physical threats to the infrastructure that support NASA missions.
- n. Threats against NASA personnel.
- o. Information pertaining to the ownership or concealment by individuals or groups of caches of firearms, explosives, or other implements of war when it is believed that their intended use is for other than legal purposes.
- p. Information concerning individuals who are perceived to be acting irrationally in their efforts to make personal contact with Government officials; information concerning anti-American or anti-U.S. Government demonstrations abroad; information concerning anti-American and anti-U.S. Government demonstrations in the United States, involving serious bodily injury or destruction of property; or an attempt or credible threat to commit such acts to further political, social, or economic goals through intimidating and coercive tactics.

2.12.4 The CCPS/CCS will maintain statistics for areas identified in Appendix C, Property Loss and Incident Details. This information will be sent to the AA, OPS quarterly and/or as requested.

2.13 Protective Services Response to Demonstrations and Civil Disturbances

2.13.1 The primary objectives in dealing with demonstrations are to direct demonstration activity to areas outside Centers and to preserve peace while protecting the rights of demonstrators peaceably to assemble and exercise free speech. Centers with property open to the general public must consult with their Center OCC/OGC.

2.13.2 The CCPS/CCS shall make reasonable efforts to safely manage groups or crowds who have assembled. The CCPS/CCS should make appropriate liaison and coordination with local law enforcement, and/or adjacent Federal agency facilities.

2.13.2.1 The CCPS/CCS will maintain an event log, commencing at the time information is first received of a demonstration and detailing thereafter all significant events, times, places, and actions with the name of the NASA official authorizing such actions.

2.13.2.2 If demonstrators trespass onto NASA property, the CCPS/CCS will protect NASA personnel, property, and information in accordance with the law.

2.13.3 The CCPS/CCS shall ensure that the contract security force receives training in dealing with demonstrators during annual in-service training and as refresher training immediately prior to a demonstration, when possible.

2.13.3.1 Ensure that NASA Special Agents, Security Specialists, and contract Security Police Officers/Security Officers (SPOs/SOs) receive training in dealing with demonstrators during in-service training and as refresher training prior to a scheduled demonstration, when possible.

2.14 Hazardous Material Security

2.14.1 Storing certain quantities of hazardous materials may be considered chemicals of interest under the Chemical Facility Antiterrorism Standards (CFATS) program managed by the DHS. When exceeding certain threshold amounts, the storage of these chemicals may have to be reported to the DHS and also require additional site specific security requirements and plans. Complete details of the program requirements are explained in 6 C.F.R. 27 Chemical Facility Antiterrorism Standards.

2.14.2 NASA programs use many different hazardous materials in meeting mission objectives. It is imperative that the use, storage, and protection of these materials be given the highest priority necessary to ensure the safety of NASA personnel and the general public.

2.14.3 In coordination with Center safety, logistics, environmental, and transportation officials, Center Protective Services Offices shall ensure the Center develops and implements security plans specifically designed to provide the appropriate level of protection in the transportation, receipt, access, use, storage, and accountability of hazardous materials used by NASA. Security Plans will include:

- a. Review of shipping/transportation procedures to ensure appropriate precautions are in place and recommend changes and/or adjustments.
- b. Appropriate sharing of threat information associated with the targeting of hazardous materials.
- c. Establishment of Center-specific receipt, escort, and hand-off procedures.
- d. Establishment of security procedures for permanent and temporary storage/holding areas to include defining secure areas.

2.15 Investigations

2.15.1 The investigative component of Protective Services is directly related to the security and protection mission and may include inquiries into such matters as threats or occurrences of workplace violence, harassment, eligibility and suitability for HSPD-12 requirements, missing or stolen property, misuse of Government property, unauthorized access, and other violations of NASA and Center security policies.

2.15.2 The CCPS/CCS shall closely coordinate investigative activity with the appropriate internal and external organizations (e.g., OIG, CIO, Office of Human Capital, Office of the Chief Counsel, EEO, FBI, ATF, DoD, and local and state police) to ensure that cases are referred to the appropriate organization for follow-up when this is required.

2.15.3 Reports of Investigation shall be thoroughly documented. HQ, OPS will be notified of investigations of security incidents as prescribed in paragraph 2.12 of this NPR.

2.15.4 The CCPS/CCS shall coordinate the release of information concerning reported missing and stolen controlled Government property with the Center Logistics Management Division on a quarterly basis to ensure accountability of controlled property and compliance with NPR 4200.1, NASA Equipment Management Procedural Requirements.

2.16 Security Education, Training, and Awareness (SETA) Program

2.16.1 General.

2.16.1.1 The effectiveness of an individual in meeting security responsibilities is proportional to the degree to which the individual understands them.

2.16.1.2 Management and employee involvement is essential to an effective security program.

2.16.1.3 An integral part of the overall NASA security program relies on the education and training of individuals regarding their security responsibilities.

2.16.2 Responsibilities.

2.16.2.1 As a minimum, the Center Director shall ensure that adequate procedures are in place whereby all NASA

employees and contractor personnel, regardless of clearance status, are briefed annually regarding Center security program responsibilities.

2.16.2.2 The CCPS/CCS for each Center shall ensure that appropriate and knowledgeable security personnel provide and receive the applicable types of briefings or training, as described in paragraph 2.16.3.

2.16.2.3 NASA supervisors shall ensure job-related, facility-oriented security education and awareness instruction or training for newly assigned personnel are timely and properly coordinated with the CCPS/CCS.

2.16.3 Required Briefings and Training.

2.16.3.1 Initial Orientation Security Briefing. This briefing shall be given by security personnel (i.e., NASA and/or security services contractor) to acquaint new employees with local security procedures and employee responsibilities to protect personnel and to protect Government property from theft, loss, or damage. Orientation briefings should include, but are not limited to, general discussions on:

- a. Access/entry and exit control procedures and responsibilities.
- b. Property accountability responsibilities.
- c. Pilferage control.
- d. Identification of restricted areas.
- e. Use and security of identification credentials.
- f. Key and lock control procedures.
- g. Protection of CNSI and/or SBU (includes Personally Identifiable Information (PII), For Official Use Only information, other privacy act information, and sensitive operational information).
- h. Emergency reporting procedures.
- i. Reporting security violations and/or suspicious activity.
- j. Orientation to the local area and criminal trends.

2.16.3.2 Annual Security Training. This training is designed to sustain an appropriate level of awareness throughout the workforce and reinforce the security policies and procedures outlined in initial orientation training.

2.16.3.3 Supervisory Security Briefing. Security orientation briefings shall be given by the responsible supervisor or designee to each new employee and will include all security requirements and procedures for which the employee is to be specifically responsible.

2.16.3.4 Security Clearance Briefing. The CCPS/CCS will ensure the appropriate security indoctrination briefing is given to each employee prior to that employee receiving a personnel security clearance and being granted access to classified information. This briefing shall include:

- a. Execution of Classified Information Nondisclosure Agreement (SF 312 and/or SCI NDA 4414, where appropriate).
- b. General security aspects affecting employment and a summary of restrictions, obligations, and reporting requirements associated with access to CNSI that are imposed by statute or executive order.
- c. Employee reporting obligations.
- d. Security procedures for handling CNSI, classified meetings and discussions, and how to apply Need-to-Know.
- e. Standards of behavior expected of persons in sensitive positions and the responsibility of security clearance holders to report behavior and adverse information which might bear on another individual's security clearance eligibility.
- f. The most current Executive Order number and information if the briefing form has not been revised to reflect that change.

2.16.4 Annual Security Clearance Refresher Briefing. The CCPS/CCS will ensure the appropriate security clearance refresher briefing is given to all NASA personnel and contractors possessing a security clearance and performing work on NASA classified programs. Initial and annual refresher briefings are also required for individuals granted accesses to certified National Security Systems that process classified information. Clearances may be suspended or revoked for failure to complete annual training.

2.16.4.1 CNSI Custodian Briefing. The CCPS/CCS will ensure classified material custodians and any other custodians responsible for CNSI security containers, records, or facilities are given initial and annual refresher briefings by security personnel regarding their specific responsibilities for safeguarding classified information.

2.16.4.2 CNSI Termination Briefing. The CCPS/CCS will ensure security termination briefings are given to employees whose personnel security clearances are being terminated due to termination of employment, transfer to another Center, or if the individual no longer requires access to CNSI. This briefing is designed to ensure termination of all classified activity and holdings by the employees and remind them of their life-long responsibilities and penalties for unauthorized disclosure of CNSI even after termination of the clearance or employment.

2.16.4.3 The CCPS/CCS will ensure other special security training or briefings are given to employees related to SAP's, SCI, and NCI. 2.16.5 Foreign Travel Briefings. CI personnel shall conduct foreign travel briefings to NASA travelers to enhance their awareness of potential hostile intelligence, terrorist, and criminal threats in the countries to which they are traveling. These briefings must also provide defensive measures and other practical advice concerning safety measures.

a. NASA employees shall report to the Center or Agency CI Office any meetings with foreign nationals from designated countries that are held outside NASA-controlled facilities in advance of the meeting.

(1) NASA employees attending the meeting will make themselves available for intelligence threat awareness pre-briefings and debriefings in accordance with NPD 1660.1B. The Center International Visit Coordinator (IVC) can provide a list of designated countries.

2.16.6 Although the OCIO has authority for SBU policy and procedures, the Center Protective Services Office shall provide both security awareness and guidance to projects and programs regarding protection of unclassified sensitive mission information or technologies. The information provided to programs and projects will be based on industry best practices and real-life lessons learned with the Agency.

2.17 NASA OPS Functional Reviews

2.17.1 This section sets standards for establishing and maintaining an ongoing NASA OPS Functional Review Program. This program shall include the periodic review and assessment of the Information, Industrial, Personnel, Physical Security, Program Security, Emergency Management, Protective Services Contract Review, and COOP operations at all NASA Centers.

2.17.2 The objective is to ensure that each Center is implementing their Protective Services programs in accordance with all applicable NASA and Federal regulations and to identify areas that need to be addressed that are not in compliance with appropriate rules and regulations. The review will also pinpoint commendable areas of each security operation and identify areas that need additional support to complete their mission.

2.17.3 Responsibilities.

2.17.3.1 The AA, OPS is responsible for the NASA OPS Functional Review Program. The AA, OPS shall designate Agency personnel to assist in carrying out this responsibility. The means and methods for the conduct of functional reviews may include:

- a. A review of relevant Protective Services directives, guides, training material, and instructions.
- b. Interviews with the Center Director (or representative), Center Operations Director (or representative), Protective Services Contracting Officer, Protective Services representatives, and customers.
- c. Review of Information, Industrial, Emergency Management, Personnel, and Physical Security Programs.
- d. Review of various files and documents pertaining to day-to-day operations and records required to be maintained by this NPR.

2.17.3.2 A standard functional review guide/checklist will be used by the inspectors conducting the review. Each Center will be inspected at least every three years. The format for documenting findings will be set by the AA, OPS. The AA, OPS, in its oversight capacity, may schedule reviews of Centers on an as needed basis.

2.17.3.3 Each review may be adjusted to meet the coverage of the security programs in place at that particular Center.

[TOC](#)	[Preface](#)	[Chapter1](#)	[Chapter2](#)	[Chapter3](#)	[Chapter4](#)	[Chapter5](#)	[Chapter6](#)
[AppendixA](#)	[AppendixB](#)	[AppendixC](#)	[AppendixD](#)	[AppendixE](#)	[AppendixF](#)		
[AppendixG](#)	[AppendixH](#)	[ALL](#)					

| [NODIS Library](#) | [Organization and Administration\(1000s\)](#) | [Search](#) |

DISTRIBUTION:
NODIS

This Document Is Uncontrolled When Printed.

Check the NASA Online Directives Information System (NODIS) Library
to Verify that this is the correct version before use: <http://nodis3.gsfc.nasa.gov>
